UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/998,484	11/30/2001	David Carroll Challener	RPS9 2001 0152	6380

47052 7590 01/24/2006

SAWYER LAW GROUP LLP
PO BOX 51418
PALO ALTO, CA 94303

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/998,484	CHALLENER ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 01 November 2005 has been noted and made of record.

2. Claims 1-41 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to claims 1-41 have been considered but are moot in view of the new ground(s) of rejection.

4. See further rejections that follow.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1, 21, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,898,577 to Johnson, hereinafter Johnson in view of U.S. Patent Application Publication No. 2002/0083332 to Grawrock, hereinafter Grawrock.

7. As per claims 1, 21, and 41, Johnson teaches a method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) signing a phrase by a security chip of the server using an encryption key (Figure 1A [block S13A], column 6, lines 37-58, i.e. encrypting the customer's password);

(b) associating the signed phrase with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65, i.e. encrypted password is associated with customer's ID);

(c) signing the phrase with an encryption key obtained by the security chip when a request for access to the computer network is received from the remote user (Figure 1B [block S13B], column 7, lines 29-34);

(d) comparing the phrase signed with the obtained encryption key with the signed phrase associated with the remote user (Figure 1B [blocks S14B, S15B], column 7, lines 34-35, i.e. the two encrypted passwords are compared); and

(e) granting access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user (Figure 1B [block S17B], column 7, lines 35-65). Wherein the security chip is the processor of the bank server, the processor processes all processes executed on a system.

8. Johnson does not disclose wherein the encryption key is known only to the security chip.

9. Grawrock discloses wherein the encryption key is known only to the security chip (figure 2, paragraphs [0022]-[0026]).

10. It would have been obvious to one of ordinary skill at the time the invention was made to have the encryption key only known to the security chip, since Grawrock states at paragraphs [0004] and [0013]-[0016] that such a modification would transmit clear and unambiguous data to a legitimate recipient while the same data would be incomprehensible to illegitimate recipients.

11. Claims 2-20 and 22-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Grawrock as applied above, and in further view of U.S. 6,725,382 to Thompson et al., hereinafter Thompson.

12. Regarding claims 2 and 22, Johnson and Grawrock do not discloses (a1) creating a public key and a private key pair for the remote user by the security chip; and (a2) signing the phrase with the private key of the remote user by the security chip.

13. Thompson teaches wherein signing step (a) comprises:

(a1) creating a public key and a private key pair for the remote user by the security chip (Figure 5 [block 466], column 6, lines 24-26); and

(a2) signing the phrase with the private key of the remote user by the security chip (claim 10).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

15. With regards to claims 3 and 23, Johnson discloses wherein the associating step (b) further comprises:

(b1) storing the signed phrase associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33).

16. Concerning claims 4 and 24, Johnson discloses wherein the signing (c) comprises:

(c1) receiving a password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65);

(c2) sending the received password and the phrase to the security chip (Figure 1B [blocks S12B, S13B], column 7, lines 5-65);

(c4) signing the phrase with the loaded private key by the security chip (Figure 1B [block S13B], column 7, lines 29-34).

17. Thompson teaches (c3) loading the private key of the remote user (Figure 5 [block 466], column 6, lines 24-26, claim 10).

18. Concerning claims 5 and 25, Johnson teaches wherein the comparing step (d) comprises:

(dl) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user (Figure 1B [blocks S14B, S15B], column 7, lines 34-35, i.e. the two encrypted passwords are compared).

19. Concerning claims 6 and 26, Johnson teaches wherein the granting step (e) comprises:

(el) granting access to the remote user if the phrase signed with the loaded private key is the same as the stored signed phrase associated with the remote user (Figure 1B [block S17B], column 7, lines 35-65).

20. Regarding claims 7 and 27, Johnson discloses wherein the signing step (a) comprises:

(al) signing a password for the remote user by the security chip (Figure 1B [block S13B], column 7, lines 29-34).

21. Grawrock discloses wherein the private key is only known to the security chip (Figure 2, paragraphs [0022]-[0026]).

22. Johnson and Grawrock do not teach signing the password with a private key of the security chip.

23. Thompson discloses signing the password with a private key of the security chip (Figure 5 [block 466], column 6, lines 24-26, claim 10).

24. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

25. With regards to claims 8 and 28, Johnson teaches wherein the associating step (b) comprises:

(b1) associating the signed password with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65); and

(b2) storing the signed password associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33).

26. Concerning claims 9 and 29, Johnson teaches wherein the signing step (c) comprises:

(c1) receiving the password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65);

(c2) sending the received password to the security chip (Figure 1B [blocks S12B, S13B], column 7, lines 5-65);

(c4) signing the received password with the loaded private key by the security chip (Figure 1B [block S13B], column 7, lines 29-34).

27. Thompson teaches (c3) loading the private key of the remote user (Figure 5 [block 466], column 6, lines 24-26, claim 10).

28. Concerning claims 10 and 30, Johnson discloses wherein the comparing step (d) comprises:

(d1) comparing the signed received password with the stored signed password (Figure 1B [blocks S14B, S15B], column 7, lines 34-35, i.e. the two encrypted passwords are compared).

29. Concerning claims 11 and 31, Johnson teaches wherein the granting step (e) comprises:

(e1) granting access to the remote user if the signed received password is the same as the stored signed password (Figure 1B [block S17B], column 7, lines 35-65).

30. Regarding claims 12 and 32, Johnson discloses wherein the signing step (a) comprises:

(a1) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a key of the security chip (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65, column 8, line 43to column 9, line 32).

31. Grawrock discloses wherein the private key is only known to the security chip (Figure 2, paragraphs [0022]-[0026]).

32. Johnson and Grawrock do not teach signing the password with a private key.

33. Thompson teaches signing using a private key (Figure 5 [block 466], column 6, lines 24-26, claim 10).

34. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

35. With regards to claims 13 and 33, Johnson discloses wherein the associating step (b) comprises:

(b1) associating the blob with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65); and

(b2) storing the blob associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33).

36. Concerning claims 14 and 34, Johnson teaches wherein the signing step (c) comprises:

(c1) receiving the password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65););

(c2) sending the received password and the blob associated with the remote user to the security chip (Figure 1B [block S13B], column 7, lines 29-34).

37. Thompson discloses (c3) decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password (Figure 5 [block 466], column 6, lines 24-26, claim 10).

38. Concerning claims 15 and 35, Johnson teaches wherein the comparing step (d) comprises:

(d1) comparing the stored password with the received password (Figure 1B [blocks S14B, S15B], column 7, lines 34-35).

39. Concerning claims 16 and 36, Johnson discloses wherein the granting step (e) comprises:

(e1) granting access to the remote user if the stored password is the same as the received password (Figure 1B [block S17B], column 7, lines 35-65).

40. Regarding claims 17 and 37, Johnson teaches (f) denying access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user (Figure 1B [blocks S16B], column 7, lines 5-65).

41. As per claims 18 and 38, Johnson discloses a method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(b) signing a phrase with the key of the remote user by the security chip (Figure 1A [block S13A], column 6, lines 37-58);

(c) associating the signed phrase with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65);

(c) storing the signed phrase associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33);

(d) receiving a password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65);

(e) sending the received password and the phrase to the security chip (Figure 1B [blocks S12B, S13B], column 7, lines 5-65);

(g) signing the phrase with the loaded key by the security chip (Figure 1B [block S13B], column 7, lines 29-34);

(h) comparing the phrase signed with the loaded private key with the stored signed phrase associated with the remote user (Figure 1B [blocks S14B, S15B], column 7, lines 34-35); and

(i) granting access to the remote user if the phrase signed with the loaded key is the same as the stored signed phrase associated with the remote user (Figure 1B [block S17B], column 7, lines 35-65).

42. Johnson does not disclose wherein the encryption key is known only to the security chip.

43. Grawrock discloses wherein the encryption key is known only to the security chip (figure 2, paragraphs [0022]-[0026]).

44. It would have been obvious to one of ordinary skill at the time the invention was made to have the encryption key only known to the security chip, since Grawrock states at paragraphs [0004] and [0013]-[0016] that such a modification would transmit clear and unambiguous data to a legitimate recipient while the same data would be incomprehensible to illegitimate recipients.

45. Johnson and Grawrock do not teach (a) creating a public key and a private key for the remote user by a security chip of the server; and (f) loading the private key of the remote user.

46. Thompson discloses (a) creating a public key and a private key for the remote user by a security chip of the server (Figure 5 [block 466], column 6, lines 24-26);

(f) loading the private key of the remote user (Figure 5 [block 466], column 6, lines 24-26, claim 10).

47. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

48. As per claims 19 and 39, Johnson teaches a method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) signing a password for the remote user by a security chip of the server with a key of the security chip (Figure 1A [block S13A], column 6, lines 37-58);

(b) associating the signed password with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65);

(c) storing the signed password associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33);

(d) receiving the password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65);

(e) sending the received password to the security chip (Figure 1B [blocks S12B, S13B], column 7, lines 5-65);

(g) signing the received password with the loaded key by the security chip (Figure 1B [block S13B], column 7, lines 29-34);

(h) comparing the signed received password with the stored signed password (Figure 1B [blocks S14B, S15B], column 7, lines 34-35); and

(i) granting access to the remote user if the signed received password is the same as the stored signed password (Figure 1B [block S17B], column 7, lines 35-65).

49. Johnson does not disclose wherein the encryption key is known only to the security chip.

50. Grawrock discloses wherein the encryption key is known only to the security chip (figure 2, paragraphs [0022]-[0026]).

51. It would have been obvious to one of ordinary skill at the time the invention was made to have the encryption key only known to the security chip, since Grawrock states at paragraphs [0004] and [0013]-[0016] that such a modification would transmit clear and unambiguous data to a legitimate recipient while the same data would be incomprehensible to illegitimate recipients.

52. Johnson and Grawrock do not teach the use of private keys or loading the private key of the security chip.

53. Thompson discloses the use of private keys and loading the private key of the remote user (Figure 5 [block 466], column 6, lines 24-26, claim 10).

54. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

55. As per claims 20 and 40, Johnson discloses a method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of:

(a) creating a blob for the remote user, wherein the blob comprises a password for the remote user signed with a key of a security chip of the server (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65, column 8, line 43to column 9, line 32);

(b) associating the blob with the remote user (Figure 1A [blocks S13A, S14A], column 6, line 37 to column 7, line 65);

(c) storing the blob associated with the remote user (Figure 1A [block S14A], column 3, lines 53-54, column 6, line 59 to column 7, line 4, column 8, line 43 to column 9, line 33);

(d) receiving the password from the remote user (Figure 1B [blocks S12B], column 7, lines 5-65);

(e) sending the received password and the blob associated with the remote user to the security chip (Figure 1B [blocks S12B, S13B], column 7, lines 5-65);

(g) comparing the stored password with the received password (Figure 1B [blocks S14B, S15B], column 7, lines 34-35); and

(h) granting access to the remote user if the stored password is the same as the received password (Figure 1B [block S17B], column 7, lines 35-65).

56. Johnson does not disclose wherein the encryption key is known only to the security chip.

57. Grawrock discloses wherein the encryption key is known only to the security chip (figure 2, paragraphs [0022]-[0026]).

58. It would have been obvious to one of ordinary skill at the time the invention was made to have the encryption key only known to the security chip, since Grawrock states at paragraphs [0004] and [0013]-[0016] that such a modification would transmit clear and unambiguous data to a legitimate recipient while the same data would be incomprehensible to illegitimate recipients.

59. Johnson and Grawrock do not teach using a private key to sign the password, and decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password.

60. Thompson teaches signing using a private key (Figure 5 [block 466], column 6, lines 24-26, claim 10); and

(f) decrypting the blob associated with the remote user using a public key of the security chip to obtain the stored password (Figure 5 [block 466], column 6, lines 24-26, claim 10).

61. It would have been obvious to one of ordinary skill in the art at the time the invention was made to create a key pair for a remote user, and signing the phrase with the private key of the user, since Thompson states at column 2, lines 4-62 that such a modification would add a low-cost security feature to portable devices.

Conclusion

62. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

63. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

64. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

65. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

66. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100